



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Serial No:

Filed:

For: NETWORK LEVEL ADMISSION CONTROL APPARATUS FOR A  
COMMUNICATIONS NETWORK HAVING A SUB-IP LEVEL PROTOCOL

**DECLARATION**

I, Andrew Scott Marland, of 35, avenue Chevreul, 92270 BOIS COLOMBES, France, declare that I am well acquainted with the English and French languages and that the attached translation of the French language specification and claims filed in respect of the above-identified US patent application is a true and faithful translation of that document.

All statements made herein are to my own knowledge true, and all statements made on information and belief are believed to be true; and further, these statements are made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any document or any registration resulting therefrom.

**FILED**

APR 27 2004

Date: November 14, 2003

Andrew Scott Marland

---

NETWORK LEVEL ADMISSION CONTROL APPARATUS FOR A  
COMMUNICATIONS NETWORK HAVING A SUB-IP LEVEL PROTOCOL

The invention relates to the field of communications between terminal via communications networks, and more particularly it relates to ensuring continuity of service for calls that involve networks of different types.

A call is often set up between two remote terminals via a plurality of communications networks that are connected to one another via edge routers or border routers. Setting up a call in this way generally presents no problem so long as the call is not associated with some particular level of service, or so long as continuity of service is not required in association with the call. However, this continuity of service situation is becoming less and less frequent because of the great variety of networks and network equipments.

Amongst the network equipment commonly in use and likely to coexist within a single call, mention can be made in particular of IP routers, routers with wavelength-division multiplexing such as dense wavelength-division multiplex (DWDM) devices, add-drop multiplexers (ADMs), photonic cross-connects (PXCs), or optical cross-connects (OXC).

Similarly, amongst the networks commonly in use and likely to be involved in a call, mention can be made in particular of those which belong to the first family of networks known as "packet switching" networks and those belonging to the second family of networks known as "non-packing switching" networks.

The networks of the first family make use of protocols at level 3 in the open systems interconnection (OSI) layer model (also known as IP level protocols, or more simply Internet protocols (or IPs)). These constitute that which is commonly called the Internet.

Networks of the second family make use of protocols at level 2 in the OSI layer model (also known as sub-IP level protocol). The second family can also be

subdivided into at least three sub-families. A first sub-family is constituted by networks using space-division switching, a second sub-family is constituted by networks using time-division multiplexing (TDM), as for example the synchronous optical network (SONET) and the synchronous digital hierarchy (SDH) network, and a third subfamily is constituted by networks using wavelength-division multiplexing (WDM).

In order to enable calls to be set up via different IP networks (belonging to the first family), proposals have been made to connect each network management system (NMS) which manages the equipment of an IP network to apparatus for controlling network level admission. On receiving a request to transfer, via its own network, a call associated with at least one service criterion and specifying another IP network connected to its own IP network, such control apparatus serves to verify whether there are available resources that are capable of satisfying the service criterion(a) associated with the call to be transferred. Thus, so long as such resources exist, the control apparatus can in turn forward the call transfer request to the control apparatus connected to the network management system managing the equipment of the designated IP network, so as to enable it to perform optional verification within its own IP network.

The term "request to transfer a call via a network" is used herein to designate the fact of using a first network to establish a "bridge" between two other networks, making available certain resources of one of the links within the first network.

By means of this type of control apparatus, it is thus possible to guarantee the continuity and the quality of service associated with a call when the IP networks involved in the call are different. However, it is also possible to guarantee security of service to a subscriber, where security of service consists in authenticating and/or encrypting a call.

However, there does not exist any known solution enabling continuity and quality of service to be guaranteed together with optional security of service associated within a single call when the call is set up  
5 over networks of different types, i.e. belonging to different sub-families of the second family (known as the sub-IP family) or belonging to different families.

An object of the invention is thus to remedy that drawback.

10 To this end, the invention provides apparatus dedicated to controlling network level admission for a set of communications networks comprising a first network with a protocol at sub-IP level (i.e. belonging to the second above-specified family), including border routers  
15 interconnected by links associated with resources of known characteristics and managed by a first network management system (NMS).

The connection apparatus is characterized by the fact that it comprises control means that firstly are fed  
20 by the network management system with data representative of the links between the border routers of the sub-IP first network and the associated resources, and that secondly, on receiving a request to transfer a call via the sub-IP first network, which call is associated with  
25 at least one service criterion and designates a second communications network that is connected to the sub-IP first network and that is of a different type (IP or sub-IP), are capable of determining from the received data whether available network resources exist that satisfy  
30 the service criterion(a) associated with the call to be transferred, and if so of forwarding the call transfer request to another control apparatus connected to the network management system (NMS) managing the designated second network, with said resources being booked only if  
35 there exist in each network involved by said call available resources that satisfy said service criterion.

It is thus possible to guarantee continuity of service and quality of service and possibly also security of service (encryption and/or authentication) associated with a call even when setting up the call involves  
5 networks of different types, i.e. belonging to different families or to different sub-families of the second family.

The service criterion is preferably selected from a group comprising at least quality of service, ability to  
10 protect/restore a link, and security of service. Ability to protect/restore a link is typically an indication of a guaranteed minimum delay for making protection/restoration resources available in the event of a fault in the network.

Also preferably, the control means may be arranged in such a manner as to store the received data in a memory in the form of a connectivity matrix between the various border routers of the sub-IP first network (it is  
15 this memory which is consulted in order to determine whether resources sufficient for the desired service are  
20 available in the sub-IP network).

In addition, the control means of the apparatus of the invention are preferably capable of being coupled to other control apparatus connected to the network  
25 management system (NMS) managing a third communications network connected to the sub-IP first network and of a different type (IP or sub-IP), and from which the call transfer request comes.

The invention also relates to network equipment,  
30 such as server, suitable for being connected to a network management system (NMS) managing a communications network using a protocol at sub-IP level and fitted with network level admission control apparatus of the type specified above.

35 Most particularly, although not exclusively, the invention applies to sub-IP communications networks selected from networks using space-division switching,

WDM networks, TDM networks, and in particular SONET and SDH networks, and generalized multiprotocol label switching (GMPLS) networks.

Other characteristics and advantages of the invention appear on examining the following detailed description and the sole accompanying figure which is a diagram showing an example of a communications installation fitted with control apparatus of the invention. This figure can contribute not only to describing the invention, but can also contribute to defining it, where appropriate.

The communications installation shown by way of example in the sole figure comprises three communications networks of different types. More precisely, in this example, the installation comprises firstly a first public data network using a protocol at level 3 of the OSI model (IP level protocol), referred to below as the first IP network (NIP1), a second public data network likewise using protocol at level 3 of the OSI model, referred to below as the second IP network (NIP2), and optionally of a type that is different from NIP1, and a third public data network using protocol at level 2 of the OSI model (i.e. a protocol at sub-IP level), referred to below as the sub-IP network (NSIP).

For example, the sub-IP network NSIP is a time-division multiplexed (TDM) network such as a SONET or an SDH network, for example. However, it could be any other type of level 2 sub-IP network, such as, for example, a network using space-division switching, or a WDM network, or a sub-IP network at so-called level "2.5", such as a GMPLS network.

The first IP network NIP1 is managed by a network management system (NMS1) of the NMS type coupled to a "network level admission control" server S1 also referred to as a network level admission controller. Each time this server S1 receives a request to transfer a call via the first IP network NIP1, the call being associated with

at least one service criterion and designating another network (in this case NSIP) connected to the first IP network NIP1, the server S1 verifies whether there exist available network resources associated with the various  
5 previously-established links (established by NMS1) within the first IP network NIP1 between its different routers and satisfying the service criteria(on) associated with the call to be transferred, where the routers may be of the edge router type ER1 or of the border router type  
10 BR1.

The second IP network NIP2 is managed by a network management system (NMS2) of the NMS type, coupled to a network level admission control server S2 that is used, each time it receives a request to transfer a call via  
15 the second IP network NIP2 in association with at least one service criterion and designating another network connected to the second IP network NIP2, to verify whether available network resources exist in association with the various previously-established links  
20 (established by NMS2) within the second IP network NIP2 between its different routers and satisfying the criteria(on) associated with the call to be transferred, which routers may be of the edge router type ER2 or of the border router type BR2.

25 The term "service criterion" is used herein to mean any matter relating to the service associated with a call, in particular quality of service or ability to ensure service continuity (also referred to as protection/restoration) in the event of a problem  
30 occurring on a link, or indeed security of service.

Quality of service (QoS) is defined by the characteristics of a resource, such as, for example, the passband on offer or the quality of service level (gold, silver, or bronze) on offer. These quality of service  
35 levels are the result of classification performed on the basis of a certain number of parameters such as passband, delay, jitter, losses, and the like.

Continuity of service is defined by parameters such as the ability to provide protection from discontinuity of service. Specifically, while data is being transferred, it is conventional practice in the event of an "interruption" to require protection/restoration to be put into place within less than 50 milliseconds (ms), for example.

Security is the ability to encrypt and/or authenticate a connection between two points in a connection matrix. It is recalled at this point that security is considered as being a network resource. Furthermore, it is the NMS<sub>i</sub> which is in charge of informing the control server S<sub>i</sub> of the possibility of encrypting and/or authenticating a call between two points of the connection matrix.

Each NMS<sub>i</sub> of the IP network NIP<sub>i</sub> (in this case  $i = 1$  or 2) supplies the corresponding control server S<sub>i</sub> in static manner (in particular during pre-operational stages) with data representative of the links established between the various edge routers ER<sub>i</sub> and border routers BR<sub>i</sub> of the IP network NIP<sub>i</sub> and of the resources associated with these links. This data subsequently makes it possible for the control server S<sub>i</sub> to memorize the occupation states of resources in its own IP network as a function of received service requests. Furthermore, the NMS<sub>i</sub> regularly informs the control server S<sub>i</sub> in such a manner as to enable it to keep its knowledge about the states of resources in correspondance with the real resources of the IP network. Thus, each control server S<sub>i</sub> knows at all times which resources are available in the IN network NIP<sub>i</sub> that it controls.

The sub-IP network NSIP is managed by a network management system (NMS3) of the NMS type coupled to network level admission control apparatus D, in this case included in a control server S3 connected to the control servers S1 and S2 of the first and second IP networks NIP1 and NIP2.



Furthermore, the sub-IP network NSIP is connected to the border routers BR<sub>i</sub> of the first and second IP networks NIP1 and NIP2 via at least some of its own border routers BR3-k (in this case k = 1 or 2).

5       The control apparatus D of the invention comprises a memory M fed by the NMS3 of the sub-IP network NSIP with network data representative of the links established between the various border routers BR3-k (in this case k = 1 or 2) of the sub-IP network NSIP and of the resources  
10 associated with these links. It is important to observe that this feeding of data to the memory takes place in an off-line type mode, independently of requests to verify the availability of resources or calls. As mentioned above, data is fed during a pre-operational stage, and  
15 also in real time throughout the lifetime of the network in question.

Furthermore, some of the network data fed to the memory M may specify a management mode applied by the server NMS3 to a link. Such management modes include in  
20 particular virtual private network (VPN) mode, optical VPN mode, and Internet protocol security (IPSec) mode.

The memory M also stores restoration data defining the network resources that are intended to replace other network resources in the event of a problem.

25       The data is preferably stored in the memory M in the form of a connectivity matrix defining all of the links established between the various border routers BR3-k of the sub-IP network NSIP, and the resources associated with these links together with their characteristics and  
30 their respective availability states, and also the restoration links and the associated resources.

The control apparatus D of the invention also comprises a control module CM coupled to the memory M and serving on each occasion it receives a request to  
35 transfer a call via the sub-IP network NSIP in association with at least one service criterion and designating another network (in this case NIP1 or NIP2)

connected to the sub-IP network NSIP, to verify whether there exist available resources associated with the various previously-established links within the sub-IP network NSIP between its border routers BR3-k which  
5 satisfy the service criteria(on) associated with the call to be transferred.

The control apparatus D is capable of taking account of signaling specific to sub-IP networks coming from a multimedia call server (MMCS) or from some other control  
10 module (or control server Si) of a neighboring network to which its sub-IP network is connected. It is also capable of taking account of protection/restoration data dedicated to the sub-IP networks and information coming from two-directional communications matrices.

15 The control module CM and possibly also the memory M may be implemented in the form of electronic circuits ("hardware"), software or computer modules ("software"), or a combination of hardware and software.

An example of the use of the communications  
20 installation shown in the sole figure is described below. In this example, it is assumed that a first communications terminal T1 seeks to exchange data with a second communications terminal T2, the data satisfying two service criteria, e.g. it is of the multimedia type  
25 and requires continuity of service to be ensured.

It is also assumed that the first and second terminals T1 and T2 are connected to public telephone networks (not shown) e.g. of the public land mobile network (PLMN) type such as a UMTS network or an i-Mode  
30 network. However, in a variant, they could be connected to a network of the public switched telephone network (PSTN) type or even directly to an IP network.

It is also assumed that the terminals T1 and T2 are mobile telephones. However they could be constituted,  
35 for example, by fixed or portable computers, fixed telephones, personal digital assistants (PDAs), or indeed

any type of communications terminal capable of exchanging data with another terminal.

The first terminal T1 initially sends a request to its own telephone network UMTS1 requesting that a call be  
5 set up with the second terminal T2 in order to exchange multimedia data with continuity of service being ensured. The network UMTS1 then initiates a procedure for determining whether the second terminal T2 is available, and if so the path that will enable the call to be set up  
10 with said second terminal T2 while satisfying both of the required service criteria.

To do this, it interrogates its own server MMCS1 which acts at call signaling level in order to make sure that the two terminals T1 and T2 and the services  
15 associated therewith are compatible prior to attempting to establish a connection (there is no point in trying to establish a connection if the remote terminal (in this case T2) is busy or if the service requested by terminal T1 is not available, for example).

In the example described, it is assumed that the server MMCS1 has used a call-level signaling procedure to determine that the second terminal T2 is available and that it is available for the service requested by the first terminal T1. Consequently, it needs to use a  
25 connection-level signaling procedure to initiate verification of resource availability. To do this, it makes the connection to the control server S1 of the first IP network NIP1 in order to request it to verify whether it has available resources that satisfy the two  
30 service criteria requested by the first terminal T1 and enabling it to transfer the call towards the sub-IP network NSIP. In the example shown, by interrogating its connectivity matrix, the control server S1 observes that some of the resources of the link established between the  
35 edge router ER1 and the border router BR1 satisfy both requested service criteria.

Knowing that its IP network NIP1 is connected to the sub-IP network NSIP, the control server S1 forwards to its control server S3 the request to verify the availability of resources satisfying both service  
 5 criteria requested by the first terminal T1 and enabling the call to be transferred to the second IP network NIP2.

This verification request is processed by the control module CM of the control apparatus D installed in the control server S3. The control module CM then  
 10 interrogates the connectivity matrix stored in the memory M and, in the example shown, discovers that certain resources of the link established between the border routers BR3-1 and BR3-2 satisfy both requested service criteria.

Knowing that its own sub-IP network NSIP is connected to IP network NIP2, the control module CM instructs the control server S3 to forward to the control server S2 of the second IP network NIP2 the request to verify the availability of resources satisfying both  
 20 service criteria requested by the first terminal T1 and enabling the call to be transferred to the network UMTS2.

In the example shown, the control server S2 interrogates its own connectivity matrix and determines that certain resources of the link established between  
 25 the border router BR2 and the edge router ER2 satisfy both requested service criteria.

When resources are available, it is preferably not necessary for the control server S2 to warn the server MMCS2 of the network UMTS2. It is preferable that such a  
 30 warning should be sent to the server MMCS1 in the event of resources not being available. Under such circumstances, the server MMCS1 then informs the server MMCS2 that the connection cannot be established.

In the example shown, since resources are available  
 35 in all three transfer (or transit) networks involved (NIP1, NSIP, and NIP2), the server MMCS2 informs the server MMCS1 which in turn informs the network UMTS1.

Naturally, when the first terminal T1 is directly connected to the IP network NIP1, the server MMCS1 informs T1 directly that it can connect with the second terminal T2. This terminates the procedure for verifying  
5 resource availability.

When resources satisfying both service criteria are available within the three networks involved in this case (NIP1, NSIP, and NIP2), resource reservation or booking can then be performed within each network and the  
10 connection between the first and second terminals T1 and T2 can be established via the edge router ER1 and the border router BR1 of the first IP network NIP1, the border routers BR3-1 and BR3-2 of the sub-IP network NSIP, and the border router BR2 and the edge router ER1  
15 of the second IP network NIP2.

The procedure for setting up the call has then terminated and the two terminals T1 and T2 can begin to exchange multimedia data with the assurance of benefiting from continuity of service throughout the duration of the  
20 call. In the event of a problem in any one of the links, they are guaranteed that the transfer network concerned (NIP1, NSIP, or NIP2) will immediately make equivalent resources available to them. In other words, the invention ensures that the continuity of service  
25 associated with a call is indeed ensured throughout the path connecting a calling terminal to a called terminal, and that this occurs regardless of the number of transfer (or transit) networks involved.

The invention is not limited to the embodiments of  
30 the installation, control apparatus, and control server described above, merely by way of example, but covers any variant that the person skilled in the art might imagine within the ambit of the following claims.

Thus, the invention is neither limited to the  
35 example combination of telephone networks and data networks shown, nor is it limited to the number of networks described, providing at least two data networks

are of different types and at least one of them is a sub-IP network.